

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**



2161

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Shinji KIKUCHI

Appln. No.: 09/964,498

Group Art Unit: 2161

Confirmation No.: 2543

Examiner: Unknown

Filed: September 28, 2001

For: ELECTRONIC COMMERCE TRANSACTION AUDIT SYSTEM, ELECTRONIC COMMERCE TRANSACTION AUDIT METHOD, AND STORAGE MEDIUM RECORDING ELECTRONIC COMMERCE TRANSACTION AUDIT PROGRAM THEREON

RECEIVED
NOV 21 2001
Technology Center 2100

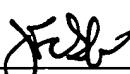
SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

Respectfully submitted,


J. Frank Osha
Registration No. 24,625

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, D.C. 20037-3213
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

Enclosures: Japanese 2000-298939

Date: NOV 21 2001



日本国特許庁
JAPAN PATENT OFFICE

S. Kikuchi
09/964,498
Filed 9/28/01
Q66458
10f1

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2000年 9月29日

出願番号
Application Number:

特願2000-298939

出願人
Applicant(s):

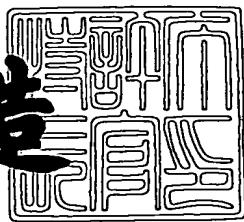
日本電気株式会社

RECEIVED
NOV 21 2001
Technology Center 2100

2001年 8月 3日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3067944

【書類名】 特許願

【整理番号】 65900019

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

【氏名】 菊地 伸治

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100082935

【弁理士】

【氏名又は名称】 京本 直樹

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100082924

【弁理士】

【氏名又は名称】 福田 修一

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100085268

【弁理士】

【氏名又は名称】 河合 信明

【電話番号】 03-3454-1111

【手数料の表示】

【予納台帳番号】 008279

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9115699

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子商取引監査システム、電子商取引監査方法及び電子商取引監査プログラムを記録した記録媒体

【特許請求の範囲】

【請求項1】 電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する複数の電子公証手段がネットワークを介して接続され、当該複数の電子公証手段が、前記記録・保存されている全ての交換メッセージの相互公証を取り合うことを特徴とする電子商取引監査システム。

【請求項2】 前記複数の電子公証手段で記録・保存された全ての交換メッセージを自動的に収集するとともに、当該収集された全ての交換メッセージの信頼性を検証することにより、ネットワーク領域全体で起こった事象を確定するトランザクションログ収集手段をさらに備えたことを特徴とする請求項1に記載の電子商取引監査システム。

【請求項3】 前記トランザクションログ収集手段で検証・確定されたネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査するログ解析手段をさらに備えたことを特徴とする請求項2に記載の電子商取引監査システム。

【請求項4】 前記トランザクションログ収集手段で検証・確定されたネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査するログ解析手段をさらに備えたことを特徴とする請求項2に記載の電子商取引監査システム。

【請求項5】 前記トランザクションログ収集手段で検証・確定されたネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査するログ解析手段をさらに備えたことを特徴とする請求項2に記載の電子商取引監査システム。

【請求項6】 前記ログ解析手段での監査の結果を電子商取引エンティティ

の識別子と対応づけて記録する累積評価管理手段と、

電子商取引エンティティの識別子を指定した監査情報の提供要求があると、前記累積評価管理手段から当該識別子と対応づけて記録された監査の結果を取り出し、監査情報として提供する監査情報サービス手段とをさらに備えたことを特徴とする請求項3乃至5のいずれかに記載の電子商取引監査システム。

【請求項7】 電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存するトランザクションログ記憶手段と、

前記トランザクションログ記憶手段により記録・保存された全ての交換メッセージの公証を他の電子公証装置に要求するとともに、当該要求に対する応答を前記他の電子公証装置から受理する公証手段と、

前記公証手段により受理された応答を記憶するトランザクション証明記憶手段とを備えたことを特徴とする電子公証装置。

【請求項8】 ネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査するログ解析手段を備えたことを特徴とする電子商取引監査装置。

【請求項9】 ネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求ることにより、各電子商取引エンティティの応答反応能力を監査するログ解析手段を備えたことを特徴とする電子商取引監査装置。

【請求項10】 ネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査するログ解析手段を備えたことを特徴とする電子商取引監査装置。

【請求項11】 電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する複数の電子公証手段が、ネットワークを介して、前記記録・保存されている全ての交換メッセージの相互公証を取り合うことを特徴とする電子商取引監査方法。

【請求項12】 前記複数の電子公証手段とは独立に設けられた評価手段が、前記複数の電子公証手段で記録・保存された全ての交換メッセージを自動的に

収集するとともに、当該収集された全ての交換メッセージの信頼性を検証することにより、ネットワーク領域全体で起こった事象を確定することを特徴とする請求項11に記載の電子商取引監査方法。

【請求項13】 前記評価手段が、さらに、前記検証・確定されたネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査することを特徴とする請求項12に記載の電子商取引監査方法。

【請求項14】 前記評価手段が、さらに、前記検証・確定されたネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査することを特徴とする請求項12に記載の電子商取引監査方法。

【請求項15】 前記評価手段が、さらに、前記検証・確定されたネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査することを特徴とする請求項12に記載の電子商取引監査方法。

【請求項16】 前記評価手段が、さらに、前記監査の結果を電子商取引エンティティの識別子と対応づけて記録しておき、電子商取引エンティティの識別子を指定した監査情報の提供要求があると、当該識別子と対応づけて記録された監査の結果を取り出し、監査情報として提供することを特徴とする請求項13乃至15のいずれかに記載の電子商取引監査方法。

【請求項17】 電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する第1のステップと、

前記第1のステップで記録・保存された全ての交換メッセージの公証を他の電子公証装置に要求する第2のステップと、

前記第2のステップでの要求に対する応答を前記他の電子公証装置から受理する第3のステップと、

前記第3のステップで受理された応答を記憶する第4のステップとを含むこと

を特徴とする電子公証方法。

【請求項18】 ネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査することを特徴とする電子商取引監査方法。

【請求項19】 ネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査することを特徴とする電子商取引監査方法。

【請求項20】 ネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査することを特徴とする電子商取引監査方法。

【請求項21】 電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する第1の処理と、

前記第1の処理で記録・保存された全ての交換メッセージの公証を他の電子公証装置に要求する第2の処理と、

前記第2の処理での要求に対する応答を前記他の電子公証装置から受理する第3の処理と、

前記第3の処理で受理された応答を記憶する第4の処理と、

をコンピュータに実行させるプログラムを記録したことを特徴とする記録媒体。

【請求項22】 ネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査する処理をコンピュータに実行させるプログラムを記録したことを特徴とする記録媒体。

【請求項23】 ネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査する処理をコンピュータに実行させるプログラムを記録したことを特徴とする記録媒体。

【請求項24】 ネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査する処理をコンピュータに実行させるプログラムを記録したことを特徴とする記録媒体。

【請求項25】 請求項21乃至24のいずれかに記載の前記プログラムを複数の部分に分割して該複数の部分をそれぞれ複数の記録媒体に記録してなる記録媒体群。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークに接続された計算機により実現される電子商取引の環境下で、各参加団体のメッセージ交換用の計算機が電子商取引に関連する各種仕様規定を満足して実装されているか、並びにその処理能力に問題がないかを監査する電子商取引監査システム、電子商取引監査方法及び電子商取引監査プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】

従来の技術例が、特開平10-93557号公報に記載されている（発明の名称「通信監査装置及び通信監査方法」）。図5は、従来発明の通信監査装置、および通信監査方法に係る暗号通信システムを示す概念図である。図5において、内部ネットワーク111は、社内ネットワーク（企業内ネットワーク）などのローカルエリアネットワークであり、例えば会社の各部署や工場、営業所などに設置された各端末を結んでいる。なお、内部ネットワーク111は、社内ネットワークに限らず、所定の組織単位あるいは管理単位のネットワークであれば良い。

【0003】

外部ネットワーク112は、内部ネットワーク111からみた外部のネットワークである。内部ネットワークを社内ネットワークとすると、外部ネットワークは社外ネットワークに相当する。外部ネットワーク112の一例としては、世界中に張り巡らされているインターネットが代表的である。

【0004】

通信監査装置120は、内部ネットワーク111に属する端末を管理対象とし、内部ネットワーク111に属する端末から社外ネットワーク112に送り出される情報を監視する。従来実施形態では、情報をパケット単位で監視するものとしている。すなわち、通信監査装置120は、パケット内に書き込まれた送信元と送信先の情報をもとに、該パケットが内部のどのユーザを送信元とし外部のどのユーザを送信先として送り出されたかを監視し、その統計情報を収集する。そして、この統計情報をもとにパケットの監査を行っている。

【0005】

図6に、従来実施形態で転送対象となるパケットの一例としてTCP/IPパケットの構造を示す。図6に示すように、パケットには、少なくとも、送信元のアドレス121、送信先のアドレス122、プロトコルの種類（ポート番号）123、データの内容124が含まれるものとする。

【0006】

なお、従来実施形態では、パケット内に送信元となるユーザ（内部のユーザ）を特定可能なデータが含まれているものとする。例えば、送信元のアドレス121で内部のユーザを特定可能とする。

【0007】

従来実施形態では内部のユーザは秘密鍵暗号を用いて情報（図6ではデータの内容124）を暗号化し通信を行うものとする。内部のユーザの使用する秘密鍵は、ユーザをキーとしてあるいはユーザとその送信相手の組をキーとして、内部ネットワーク111内で管理されているものとする。秘密鍵暗号については、池野、小山共著「現代暗号理論」電子情報通信学会編や、岡本著「暗号理論入門」共立出版株式会社等に詳しいので、ここでの説明は省略する。

【0008】

次に通信監査装置120の機能について説明する。通信監査装置120は、内部のユーザから外部への送信の状況を、パケットの送信元アドレス121と送信先アドレス122を参照して統計的処理により把握する。そして、所定の統計量が予め定められた所定の条件を満たすものになると（例えば転送パケットの累計

数がしきい値以上になると）、パケットをその本来の送信先へは転送せずに、パケット内の暗号化された情報を復号しその内容の監査を行うために該パケットを監査人（すなわち、内部の特定のユーザ）宛てに転送する。

【0009】

図7は、通信監査装置120による監査の概要を示す。図7において、ユーザAを監査人、ユーザBを内部のユーザ（例えば社員）とし、ユーザCとユーザDが外部のユーザ（例えば社外のユーザ）であるとする。

【0010】

通信監査装置120は、内部のユーザBから外部のユーザC宛てあるいはユーザD宛てのパケットを受け取ると、パケット内に記述されている送信元アドレスと送信先アドレスを調べ、送信元と送信先の組ごとにパケット量を累計して行く。

【0011】

図7では、ユーザBの通信記録として、C宛てにX回、D宛てにY回、パケット転送が行われた状態が示されている。ここで、例えば、上記所定の条件を「今受け取ったパケットをその宛先に転送すると通信回数がX（ここで $X > Y$ とする）回を越える」条件であるとする。この場合、図7の状態でユーザBからD宛てにパケットが送信されると、該パケットはこの条件を満たさないので、通信監査装置120はD宛てにパケットを送り出す（D宛ての通信回数は $Y + 1$ となる）。一方、図7の状態でユーザBからC宛てに送信されたパケットが通信監査装置120に入力されると、C宛ての通信回数は $X + 1$ にカウントアップされ、この結果、該パケットは上記条件を満たすことになるので、通信監査装置120は、該パケットをC宛てには転送せずに、監査人Aの端末宛てに転送する。

【0012】

このようにして上記パケットを転送された監査人Aは、送信元アドレス（または送信元アドレスと送信先アドレスの組）により特定される秘密鍵を用いて該パケット内の暗号化データを復号して内容を監査することができる。なお、該秘密鍵は、監査人Aの端末あるいはこれに直接接続されたサーバあるいは内部ネットワーク111内の他のサーバ装置で管理し、監査人Aの端末にて入手可能である。

ものとする。

【0013】

また、監査後、その内容に問題がないと判断された場合には、該監査人Aの端末からパケットをあらためて本来の送信先に向けて送り出すようにしても良い。あるいは、通信監査装置120内にて該パケットを識別子を付して保持しておき、該監査人Aの端末から通信監査装置120にパケットの識別子を指定して該パケットをその本来の送信先に向けて送り出すよう指示を出すようにしても良い。あるいは、該パケットの送信元に該パケットを再度その本来の送信先に向けて送り出すよう指示を出すようにしても良い。

【0014】

ここで、前記所定の条件を適宜設定することにより、監査対象を絞った効率的かつ効果的な監査を行うことができる。例えば、所定の条件を総転送回数のしきい値とすることにより、転送回数が際だって多い特定の送信元と送信先の組を持つ情報についてのみ監査対象とすることができます。

【0015】

次に、図8に、従来通信監査装置120の内部構成の一例を示す。通信監査装置120は、パケット解析部143、送信ログ取得部145、送信パケット統計処理部146、監査条件判定部147、メール発信部148を備えている。

【0016】

図8において、141はユーザBからの暗号メールを示し、142は送信されるパケットに含まれる情報の概略を示している。まず、暗号メールを受信すると、パケット解析部143でパケット内に記述された該パケットの送信元と送信先を検出する。また、必要に応じて、プロトコルの種類、データ量など、他の情報も検出する。

【0017】

次に、送信ログ取得部145は、パケットの送信元と送信先の組ごとにログを取る。ログの内容は、例えば、日時、送信元、送信先、プロトコルの種類などからなる。あるいは、データ量などを付加しても良い。

【0018】

次に、送信パケット統計処理部146は、送信ログ取得部145からの情報をもとに、パケット毎に統計処理を行う。ここでは、送信元と送信先の組ごとにパケット数を計数するものとする。なお、送信元と送信先とプロトコルの種類の組ごとに統計処理を行っても良いし、特定の種類のプロトコルについてのみ、送信元と送信先の組ごとにパケット数の計数するようにしても良いし、その他、種々の統計処理の方法が考えられる。

【0019】

なお、送信ログ取得部145を設けない構成も考えられる。この場合、パケット解析部143から直接、送信パケット統計処理部146に、必要なデータを与える。次に、監査条件判定部147は、パケット毎に行った統計処理により得られる所定の統計量が、予め定めた条件を満たすか否か判定する。

【0020】

ここでは、一例として、所定の統計量を送信回数nとし、予め定めた条件を「送信回数nがしきい値N以上であること」とする。この場合、監査条件判定部147は、暗号メールを監査するか否かを決定するためのしきい値Nと送信回数nを比較する。

【0021】

上記条件が満たされない場合（本具体例では $N > n$ である場合）には、監査すべき条件が満たされないので、該電子メールを本来の送信先に向けて外部ネットワーク112に送り出す。

【0022】

一方、上記条件が満たされる場合（本具体例では $N \leq n$ である場合）には、監査すべき条件が満たされるので、メール発信部148は、このメールを監査人Aに発信する。

【0023】

なお、通信監査装置120内では、パケットを送信するまでバッファに蓄積しておいても良いし、パケット解析部143、送信ログ取得部145、送信パケット統計処理部146、監査条件判定部147、メール発信部148の各部分でリレーして言っても良い。

【0024】

次に、具体例を用いて従来の通信監査装置120の動作例を説明する。今、図8のユーザBが暗号メールをユーザC宛てに送信したとする。ユーザBが発信した暗号メールは、パケットとして図8中の142に示すように発信元および発信先がヘッダとして付加される。

【0025】

このパケットを受け取った通信監査装置120では、パケット解析部143により該パケットがユーザBからのパケットであることと、該パケットがユーザCへ発信されていることなどを検出し、その結果を送信ログ取得部145へ送る。

【0026】

送信ログ取得部145は、送信元と送信先とを組にして、パケット送信のログを記録しておく。本具体例では、ユーザBがパケットをユーザCに送信したログを記録しておく。

【0027】

この結果を、送信パケット統計処理部146へ送り、ある特定のパケット、例えば現在送信されているパケットのこれまでの個数をカウントする。この結果をnとする。

【0028】

このnを監査条件判定部147へ送り、あるしきい値Nと比較する。このしきい値は、監査人Aが予め設定した値である。このとき、nがしきい値N未満である場合は、該パケットをユーザCに向けて外部ネットワーク112に送り出す。

【0029】

一方、nがしきい値N以上となった場合は、メール発信部148にて、ユーザBが送信した暗号メールを監査人Aへ送信する。なお、同時に、ユーザBからユーザCへのパケットの量がしきい値N以上となったことをメールにて知らせるようにしても良い。

【0030】

この結果、監査人Aは、ユーザBから出されたユーザC宛ての暗号メールを、所定の鍵で復号し内容を監査することができる。また、メール発信部148は、

ある特定の内容を持つパケット、例えば使用されていないポート番号を付加したパケットをユーザBのホストマシンへ送信する。ユーザBのホストマシンは、警告メッセージ発信部149でこの特定のパケットを受け取り、警告メッセージをユーザBが使用しているマシンのディスプレイ上に、例えば、「これより暗号化されたメールの監査を行います」というメッセージとして表示するようにしても良い。この警告メッセージは、現在使われているファイアウォールの警告システムと同様に、各ホストマシンにソフトウェアで実現可能である。

【0031】

なお、以上では、所定の統計量としてパケット数、所定の条件として「パケット数がしきい値以上になること」を一例として示したが、これに限定されるものではない。

【0032】

例えば、監査対象とする送信元の範囲、あるいは送信先の範囲、あるいは送信元と送信先の組の範囲を限定しても良い。また、上記所定条件、あるいは所定統計量、および所定条件を、送信元、あるいは送信先、あるいは送信元と送信先の組ごとに設定しても良い。

【0033】

また、上記所定の統計量を一定期間毎に求めても良い。例えば、転送パケット数を月初めにクリアし、当該月における転送パケット数としきい値を比較するようにしても良いし、その日から過去一定期間の間の転送パケット数で比較するようにしても良い。

【0034】

その他、種々変形して実施可能である。なお、以上では、監査するパケットを監査人に転送していたが、その代わりに、パケットは監査人に転送せずに、監査人にメッセージのみ転送するようにしても良い。この場合にも、監査人は、通信監査装置内に保持されているパケットを監査することができる。

【0035】

ところで、内部のユーザが、自分のホストマシンを立ち上げ、マシンにログインをすると、画面上に、例えば「本システムを使用して外部へ情報を暗号化して

送信する場合、復号して情報の内容を監査することができます。」というメッセージを表示させるようにしても良い。

【0036】

これによって、該端末のユーザに警告を与え、例えば外部に企業秘密に関わる情報を漏洩するような不正を心理的に抑え未然に防止する効果を得ることができます。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0037】

【発明が解決しようとする課題】

しかしながら、上記従来の技術には以下の問題点がある。

【0038】

第1に、従来の方式では、パケットの解析を行っているものの一つのサイトに限定された監査のみであり、その条件設定もそのサイトに閉じたものしか設定出来ない。しかし、現実の電子商取引では、メールシステム以上に複雑なメッセージ転送が存在し、2サイト間だけのメッセージ交換だけで済む場合は、むしろ少ない。このような現実の電子商取引においては、広域なネットワーク領域を捉えて、事象の検証を行う監査方法が必要であり、従来方式では実現不可能である。

【0039】

第2に、従来の方式では、システム基盤に関連する項目が主な監査対象であり、メッセージの内容を判断して、監査を行うことが出来ない。例えば、金融取引き上の不渡等が発生し得るか、否かについての監査は、単なるパケットのトレスだけではなく、メッセージの内容を正しく判断しなければ、実現不可能である。その意味で、従来方式は、現実の電子商取引での監査に利用することは出来ない。

【0040】

第3に、従来の方式では、監査人や、システム自体の信頼性保証の考え方がなく、重大な記録を漏洩し得る可能性も残されている。監査するポイントもインターネットの様な外部ネットワークと企業内の内部ネットワークの接点であり、監査人に極めて高い権限と責任を階層的に与える社会基盤的仕組みになっていると

は言えない。その為、社会的責任を持つ包括的監査よりも、特定団体責任しか持たない監査が中心になる為、電子商取引が総取引上で大きな配分比を占めるようになった場合は、極めて危険な状況を招くことになる。

【0041】

昨今、電子商取引が益々、重要な役割を担うことになり、総取引の中でも大きな位置を占めつつある。その為、電子商取引環境を厳正、厳密、且つリアルタイムに監査出来る手段が必要になって来ている。そこで、本発明は、ネットワークに接続された計算機により実現される電子商取引の環境下で、企業を始めとする各参加団体のメッセージ交換用の計算機が電子商取引に関連する各種仕様規定を満足して実装されているか、並びにその処理能力に問題がないかを監査することを目的としている。

【0042】

【課題を解決するための手段】

本発明の第1の電子商取引監査システムは、電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する複数の電子公証手段がネットワークを介して接続され、当該複数の電子公証手段が、前記記録・保存されている全ての交換メッセージの相互公証を取り合うことを特徴とする。

【0043】

本発明の第2の電子商取引監査システムは、上記第1の電子商取引監査システムにおいて、前記複数の電子公証手段で記録・保存された全ての交換メッセージを自動的に収集するとともに、当該収集された全ての交換メッセージの信頼性を検証することにより、ネットワーク領域全体で起こった事象を確定するトランザクションログ収集手段をさらに備えている。

【0044】

本発明の第3の電子商取引監査システムは、上記第2の電子商取引監査システムにおいて、前記トランザクションログ収集手段で検証・確定されたネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査するログ解析手段をさらに備えている。

【0045】

本発明の第4の電子商取引監査システムは、上記第2の電子商取引監査システムにおいて、前記トランザクションログ収集手段で検証・確定されたネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求ることにより、各電子商取引エンティティの応答反応能力を監査するログ解析手段をさらに備えている。

【0046】

本発明の第5の電子商取引監査システムは、上記第2の電子商取引監査システムにおいて、前記トランザクションログ収集手段で検証・確定されたネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査するログ解析手段をさらに備えている。

【0047】

本発明の第6の電子商取引監査システムは、上記第3乃至第5のいずれかの電子商取引監査システムにおいて、前記ログ解析手段での監査の結果を電子商取引エンティティの識別子と対応づけて記録する累積評価管理手段と、電子商取引エンティティの識別子を指定した監査情報の提供要求があると、前記累積評価管理手段から当該識別子と対応づけて記録された監査の結果を取り出し、監査情報として提供する監査情報サービス手段とをさらに備えている。

【0048】

本発明の電子公証装置は、電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存するトランザクションログ記憶手段と、前記トランザクションログ記憶手段により記録・保存された全ての交換メッセージの公証を他の電子公証装置に要求するとともに、当該要求に対する応答を前記他の電子公証装置から受理する公証手段と、前記公証手段により受理された応答を記憶するトランザクション証明記憶手段とを備えている。

【0049】

本発明の第1の電子商取引監査装置は、ネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較する

ことにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査するログ解析手段を備えている。

【0050】

本発明の第2の電子商取引監査装置は、ネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査するログ解析手段を備えている。

【0051】

本発明の第3の電子商取引監査装置は、ネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査するログ解析手段を備えている。

【0052】

本発明の第1の電子商取引監査方法は、電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する複数の電子公証手段が、ネットワークを介して、前記記録・保存されている全ての交換メッセージの相互公証を取り合うことを特徴とする。

【0053】

本発明の第2の電子商取引監査方法は、上記第1の電子商取引監査方法において、前記複数の電子公証手段とは独立に設けられた評価手段が、前記複数の電子公証手段で記録・保存された全ての交換メッセージを自動的に収集するとともに、当該収集された全ての交換メッセージの信頼性を検証することにより、ネットワーク領域全体で起こった事象を確定することを特徴とする。

【0054】

本発明の第3の電子商取引監査方法は、上記第2の電子商取引監査方法において、前記評価手段が、さらに、前記検証・確定されたネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査することを特徴とする。

【0055】

本発明の第4の電子商取引監査方法は、上記第2の電子商取引監査方法において、前記評価手段が、さらに、前記検証・確定されたネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査することを特徴とする。

【0056】

本発明の第5の電子商取引監査方法は、上記第2の電子商取引監査方法において、前記評価手段が、さらに、前記検証・確定されたネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査することを特徴とする。

【0057】

本発明の第6の電子商取引監査方法は、上記第3乃至第5のいずれかの電子商取引監査方法において、前記評価手段が、さらに、前記監査の結果を電子商取引エンティティの識別子と対応づけて記録しておき、電子商取引エンティティの識別子を指定した監査情報の提供要求があると、当該識別子と対応づけて記録された監査の結果を取り出し、監査情報として提供することを特徴とする。

【0058】

本発明の電子公証方法は、電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する第1のステップと、前記第1のステップで記録・保存された全ての交換メッセージの公証を他の電子公証装置に要求する第2のステップと、前記第2のステップでの要求に対する応答を前記他の電子公証装置から受理する第3のステップと、前記第3のステップで受理された応答を記憶する第4のステップとを含んでいる。

【0059】

本発明の第7の電子商取引監査方法は、ネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査することを特徴とする。

【0060】

本発明の第8の電子商取引監査方法は、ネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査することを特徴とする。

【0061】

本発明の第9の電子商取引監査方法は、ネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査することを特徴とする。

【0062】

本発明の第1の記録媒体は、電子商取引エンティティ間の全ての交換メッセージに時刻を統一的に打刻し記録・保存する第1の処理と、前記第1の処理で記録・保存された全ての交換メッセージの公証を他の電子公証装置に要求する第2の処理と、前記第2の処理での要求に対する応答を前記他の電子公証装置から受理する第3の処理と、前記第3の処理で受理された応答を記憶する第4の処理と、をコンピュータに実行させるプログラムを記録している。

【0063】

本発明の第2の記録媒体は、ネットワーク領域全体で起こった事象と、あらかじめ把握されるネットワーク領域全体で起こるべき事象とを比較することにより、各電子商取引エンティティにおける電子商取引の仕様準拠性を監査する処理をコンピュータに実行させるプログラムを記録している。

【0064】

本発明の第3の記録媒体は、ネットワーク領域全体で起こった事象において、要求メッセージを受け取ってから応答メッセージを戻すまでの時間を求めることにより、各電子商取引エンティティの応答反応能力を監査する処理をコンピュータに実行させるプログラムを記録している。

【0065】

本発明の第4の記録媒体は、ネットワーク領域全体で起こった事象において、異常応答発生の頻度を計算することにより、各電子商取引エンティティの異常応答処理比率を監査する処理をコンピュータに実行させるプログラムを記録してい

る。

【0066】

本発明の記録媒体群は、第1乃至第4のいずれかの記録媒体に記録された前記プログラムを複数の部分に分割して該複数の部分をそれぞれ複数の記録媒体に記録してなる。

【0067】

【発明の実施の形態】

次に本発明の第1の実施の形態について図面を参照して詳細に説明する。

【0068】

図1を参照すると、本実施の形態に係る電子商取引監査システムは、電子商取引を実施する企業群が所属するスコープを管理するスコープ取引き監視サイト3、4、および、評価サイト5、タイムスタンプサーバ21、認証・登録局22を含んで構成される。

【0069】

図1の事例で、企業A6、企業B7はスコープA1に所属し、企業C8、企業D9はスコープB2に所属するものとする。当該スコープA1では、スコープA取引き監視サイト3により、当該スコープB2では、スコープB取引き監視サイト4により、それぞれ、参加している企業名、アクセス先、サポートするサービス等が詳細に管理される。

【0070】

企業A6には、電子商取引上の各種メッセージ通信の状態管理を行う、電子商取引エンティティ11が含まれる。同様に、企業B7には電子商取引エンティティ12が、企業C8には電子商取引エンティティ13が、企業D9には電子商取引エンティティ14がそれぞれ含まれることになる。

【0071】

スコープA取引き監視サイト3は、前述電子商取引エンティティ11、12、13、14間でやり取りされる電子商取引に関するメッセージをトレースし、通信の状態管理を行う公証エンティティ15、並びに当該メッセージにより実現されるトランザクションの全履歴を管理するトランザクションログ17、並びに当

該トランザクションログ17の正当性を保証するトランザクション証明19を含んで構成される。

【0072】

同様に、スコープB取引き監視サイト4も、公証エンティティ16、並びにトランザクションログ18、並びに当該トランザクションログ18の正当性を保証するトランザクション証明20を含んで構成される。

【0073】

前述評価サイト5は、前述のトランザクションログ17、18を収集するトランザクションログ収集エージェント25、プロトコル標準収集エージェント27、前述トランザクションログ17、18を複製することにより生成されるトランザクションログ26、26'、26"、該トランザクションログ26、26'、26"を解析することにより、各企業が保有している電子商取引エンティティ11、12、13、14の監査を行うログ解析エンジン28、並びに当該ログ解析エンジン28が出す監査結果を管理する累積評価管理部31、前述ログ解析エンジン28が監査を行う際に参照するトランザクション定義A30、トランザクション定義B29、並びに、監査結果を管理する前述累積評価管理部31を使って、各企業に監査情報サービスを提供する監査情報サービス32を含んで構成される。

【0074】

次に、本実施の形態に係る電子商取引監査システムの具体的な処理手順について説明する。

【0075】

まず、スコープA1に所属する企業A6が、スコープB2に所属する企業C8と電子商取引を行う場合を例にとり、スコープA取引き監視サイト3およびスコープB取引き監視サイト4による監視の動作を説明する。

【0076】

この場合、電子商取引上の各種メッセージ通信の状態管理を行う、前述企業A6内の電子商取引エンティティ11は、最初にスコープA1を管理する前述スコープA取引き監視サイト3内の公証エンティティ15に、タイムスタンプ要求a

1を転送する。

【0077】

タイムスタンプ要求a1は、下記の様な構成を取る。

```
Time_Stamp_Request::=
Digest.Of_Message;
Entity_Identifier.Of_Sender;
Entity_Identifier.Of_Receiver;
Category.Of_Message;
Identifier.Of_Message;
Transaction_Identifier;
Invocation_Time_At_Sender;
Signature.Of_Sender;
Key_Information;
};
```

当該タイムスタンプ要求a1中のDigest.Of_Messageは、前述企業A6が、前述企業C8に転送しようとする要求メッセージa6を指定された方式でダイジェスト計算した結果値である。

【0078】

当該タイムスタンプ要求a1中のEntity_Identifier.Of_Sender、並びにEntity_Identifier.Of_Receiverは、前述電子商取引エンティティ11、前述電子商取引エンティティ13に関するアクセスポイントを意味し、国際規約団体W3C等で定められたURI(Uniform Resource Identifier)等で記述される。

【0079】

当該タイムスタンプ要求a1中のCategory.Of_Message、並びにIdentifier.Of_Messageは、転送されるメッセージの種類を特定するものである。本システムは、RosettaNetに代表される特定団体のみを対象としている訳ではない為、Category.Of_Messageでは、送付するメッセージを規定した団体の識別子が設定され、Identifier.Of_Messageでは、その団体内のメッセージ識別子が設定される。例えば、RosettaNetの場合は、前述Category.Of_Messageに

は、”RosettaNet”等の文字列が設定され、Identifier.Of_Messageには、メッセージの種類を特定するPIP番号とメッセージ種類等を組み合わせた文字列が設定されることになる。

【0080】

前述タイムスタンプ要求a1中の、Transaction_Identifier、Invocation_Time_At_Senderは、そのメッセージにより実現されるトランザクションを特定する識別子、並びに前述電子商取引エンティティ11内でのローカルな起動時刻を意味する。当該Transaction_Identifierは、本システム全体に渡り、一意な値を持つように設定され、当該トランザクションが仕様に基いた動作を実施し、完結されるまで、同じ値が維持・利用される。これには、例えば、取引監視サイトの識別子に、そのサイト内で管理される一連番号を付した識別情報等が相当する。前述ログ解析エンジン28は、このTransaction_Identifierを元に、複数メッセージの交換により実現するトランザクションの仕様準拠性を判定することになる。

【0081】

前述タイムスタンプ要求a1中のSignature.Of_Senderは、前述Digest.Of_Messageに、前述電子商取引エンティティ11の秘密鍵で署名をしたものである。対して、前述タイムスタンプ要求a1中のKey_Informationは、当該秘密鍵に対応する公開鍵証明書に関する情報である。

【0082】

前述公証エンティティ15は、前述タイムスタンプ要求a1を受理すると、システム内で正しい時刻を打刻出来る様に時刻要求a2をタイムスタンプサーバ21に転送する。

【0083】

前述タイムスタンプサーバ21は、前述時刻要求a2を受けると、妥当な表現形式で時刻値応答a3を、前述公証エンティティ15に転送する。

【0084】

前述公証エンティティ15は、前述時刻値応答a3を受理後、前述のタイムスタンプ要求a1と結合して、下記の様な構成の受領確認a4を作成し、トランザクションログ17に、時間順序を維持しながら格納する。

【0085】

前述受領確認 a 4 は、下記の様な構成を取る。

```
Recieve_Confirmation ::= {  
    Time_Stamp_Request;  
    Time_Stamp_Value;  
    Signature_Of_Notary_Entity;  
    Key_Information;  
};
```

前述受領確認 a 4 内の Time_Stamp_Request は、前述タイムスタンプ要求 a 1 と等価である。 Time_Stamp_Value は、前述時刻値応答 a 3 の値と等価である。

【0086】

前述受領確認 a 4 内の Signature_Of_Notary_Entity は、前述 Time_Stamp_Request と前述 Time_Stamp_Value とを組み合わせて、前述公証エンティティ 15 の秘密鍵で署名をしたものである。対して、前述受領確認 a 4 内の Key_Information は、当該公証エンティティ 15 の秘密鍵に対応する公開鍵証明書に関する情報である。

【0087】

前述公証エンティティ 15 は、その後、前述受領確認 a 4 と同じ構成を持ち前述タイムスタンプ要求 a 1 に対応したタイムスタンプ応答 a 5 を前述電子商取引エンティティ 11 に戻す。

【0088】

タイムスタンプ応答 a 5 は、下記の様な構成を取る。

```
Time_Stamp_Response ::= {  
    Time_Stamp_Request;  
    Time_Stamp_Value;  
    Signature_Of_Notary_Entity;  
    Key_Information;  
};
```

前述タイムスタンプ応答 a 5 を受けた、前述電子商取引エンティティ 11 は、

転送先である企業C 8内の電子商取引エンティティ13に転送しようとする要求メッセージa6を送付する。その場合、トランザクション特定識別子であるTransaction_Identifierが当該メッセージa6に含まれることになる。その際、前述のタイムスタンプ応答a5は、特に転送される必要はない。

【0089】

企業C 8内の前述電子商取引エンティティ13が当該要求メッセージa6を受理すると、スコープB 2を管理する前述スコープB取引き監視サイト4内の公証エンティティ16に、タイムスタンプ要求a7を転送する。

【0090】

タイムスタンプ要求a7は、前述タイムスタンプ要求a1と同じ構成で、下記の様な構成を取る。

```
Time_Stamp_Request ::= {
  Digest_0f_Message;
  Entity_Identifier_0f_Sender;
  Entity_Identifier_0f_Receiver;
  Category_0f_Message;
  Identifier_0f_Message;
  Transaction_Identifier;
  Invocation_Time_At_Sender;
  Signature_0f_Sender;
  Key_Information;
};
```

当該タイムスタンプ要求a7中のDigest_0f_Messageは、前述企業A 6が、前述企業C 8に転送した要求メッセージを指定された方式でダイジェスト計算した結果値である。

【0091】

前述タイムスタンプ要求a7中のTransaction_Identifierは、前述要求メッセージa6が実現するトランザクションを特定する識別子を意味する。これは、前述の通り、本システム全体に渡り、一意な値を持つように設定されるので、前述

タイムスタンプ要求 a 1 中の *Transaction_Identifier* と同じ値を持つ。

【0092】

前述タイムスタンプ要求 a 7 中の *Invocation_Time_At_Sender* は、前述電子商取引エンティティ 13 内でのローカルな起動時刻を意味する。

【0093】

前述タイムスタンプ要求 a 7 中の *Signature_Of_Sender* は、前述 *Digest.Of_Message* に、前述電子商取引エンティティ 13 の秘密鍵で署名をしたものである。従って、前述タイムスタンプ要求 a 1 中の *Signature_Of_Sender* とは異なる値になる。対して、前述タイムスタンプ要求 a 7 中の *Key_Information* は、当該秘密鍵に対応する公開鍵証明書に関する情報であり、これも前述タイムスタンプ要求 a 1 中の *Key_Information* とは値が異なることになる。

【0094】

前述公証エンティティ 16 は、前述タイムスタンプ要求 a 7 を受理すると、システム内で正しい時刻を打刻出来る様に時刻要求 a 8 を前述タイムスタンプサーバ 21 に転送する。

【0095】

前述タイムスタンプサーバ 21 は、前述時刻要求 a 8 を受けると、妥当な表現形式で時刻値応答 a 9 を、前述公証エンティティ 16 に転送する。

当該公証エンティティ 16 は、前述時刻値応答 a 9 を受理後、前述のタイムスタンプ要求 a 7 と結合して、下記の様な構成の受領確認 a 10 を作成し、トランザクションログ 18 に、時間順序を維持しながら格納する。

【0096】

前述受領確認 a 10 は、前述受領確認 a 4 と同じ構成である。前述受領確認 a 10 内の *Time_Stamp_Request* は、前述タイムスタンプ要求 a 7 と等価である。 *Time_Stamp_Value* は、前述時刻値応答 a 9 の値と等価である。

【0097】

前述公証エンティティ 16 は、その後、前述受領確認 a 4 と同じ構成を持ち前述タイムスタンプ要求 a 7 に対応したタイムスタンプ応答 a 11 を前述電子商取引エンティティ 13 に戻す。

[0098]

その後、前述電子商取引エンティティ 1 3 は、要求された処理を実施し、更に連鎖的に生じる要求メッセージを他の企業内の電子商取引エンティティに送付するか、前述要求メッセージ a 6 に対する応答メッセージを前述電子商取引エンティティ 1 1 に戻すか、を行うことになる。前述電子商取引エンティティ 1 3 が、どの様な応答メッセージを転送するかについては、プロトコル標準管理リポジトリサイト A 2 4、プロトコル標準管理リポジトリサイト B 2 3 等に管理されているプロトコル標準により定められている。

[0 0 9 9]

前述公証エンティティ 15 は、前述トランザクションログ 17 に前述受領確認 a 4 を時間順序を維持しながら格納する。加えて、前述公証エンティティ 16 も、前述トランザクションログ 18 に前述受領確認 a 10 を時間順序を維持しながら格納する。

[0 1 0 0]

ところで、前述公証エンティティ 15、16 は互いに公証処理上の整合性を保証する必要がある為、前述公証エンティティ 15、16 を始めとする複数の公証エンティティ間であらかじめ決められた時間間隔△毎にトランザクションログの相互公証を取り合う。

[0 1 0 1]

例えば、公証エンティティ 15 は、時間間隔 Δ 毎に、前述トランザクションログ 17 から前回の最終時刻 T 以後の、且つ最古の前述受領確認 a_4 から、時刻 ($T + \Delta$) 迄の前述受領確認 a_4 を総べて取り出し、それらを含むトランザクションリスト a_{12} を生成する。

その後、公証エンティティ1-5はメモリ上に管理されている、前述最終時刻T

を、時刻 (T + Δ) に更新する。当該Receive_Confirmationの配列の各々は、前述の受領確認 a 4 に相当することになる。

【0102】

その後、当該トランザクションリスト a 1 2 を元に、トランザクション証明要求 a 1 3 を生成する。当該トランザクション証明要求 a 1 3 は、下記の様な構成を取る。

```
Transaction_Notary_Request::= {
  Transaction_List;
  Entity_Identifier_Of_Sender;
  Entity_Identifier_Of_Receiver;
  Invocation_Time_At_Sender;
  Signature_Of_Sender;
  Key_Information;
};
```

前述トランザクション証明要求 a 1 3 内のEntity_Identifier_Of_Senderは、前述公証エンティティ 1 5 に関するアクセスポイントを意味し、国際規約団体 W 3 C 等で定められた U R I (Uniform Resource Identifier) 等で記述される。対して、当該トランザクション証明要求 a 1 3 のEntity_Identifier_Of_Receiver は、当該前述公証エンティティ 1 5 と相互公証を取り合う複数の他公証エンティティの一つに関するアクセスポイントを意味し、これも、国際規約団体 W 3 C 等で定められた U R I (Uniform Resource Identifier) 等で記述される。

【0103】

前述トランザクション証明要求 a 1 3 内のInvocation_Time_At_Senderは、前述公証エンティティ 1 5 内でのローカルな起動時刻を意味する。

【0104】

前述トランザクション証明要求 a 1 3 内のSignature_Of_Senderは、前述Transaction_Listを決められた方式でダイジェスト計算し、前述公証エンティティ 1 5 の秘密鍵で署名をしたものである。対して、前述トランザクション証明要求 a 1 3 内のKey_Informationは、当該秘密鍵に対応する公開鍵証明書に関する情報

である。

【0105】

前述公証エンティティ15と相互公証を取り合う複数の他公証エンティティの一つが、スコープB2内の前述公証エンティティ16である場合を考える。当該公証エンティティ16が前述トランザクション証明要求a13を公証エンティティ15から受理すると、それに署名を施し、トランザクション証明応答a14を公証エンティティ15に戻す。当該トランザクション証明応答a14は、下記の様な構成を取る。

```
Transaction_Notary_Response ::= {
  Transaction_Notary_Request;
  Entity_Identifier_Of_Sender;
  Entity_Identifier_Of_Receiver;
  Invocation_Time_At_Sender;
  Signature_Of_Sender;
  Key_Information;
};
```

前述トランザクション証明応答a14内のEntity_Identifier_Of_Receiverは、前述公証エンティティ15に関するアクセスポイントを意味し、国際規約団体W3C等で定められたURI(Uniform Resource Identifier)等で記述される。対して、当該トランザクション証明要求a13のEntity_Identifier_Of_Senderは、前述公証エンティティ15と相互公証を取り合う複数の他公証エンティティの一つに関するアクセスポイントを意味し、これも、国際規約団体W3C等で定められたURI(Uniform Resource Identifier)等で記述される。

【0106】

前述トランザクション証明応答a14内のInvocation_Time_At_Senderは、前述公証エンティティ16内でのローカルな起動時刻を意味する。

【0107】

前述トランザクション証明応答a14内のSignature_Of_Senderは、前述トランザクション証明要求a13の構造Transaction_Notary_Requestそのものを、決

められた方式でダイジェスト計算し、前述公証エンティティ16の秘密鍵で署名をしたものである。対して、前述トランザクション証明応答a14内のKey_Informationは、当該秘密鍵に対応する公開鍵証明書に関する情報である。

【0108】

前述公証エンティティ15は、前述トランザクション証明応答a14を受理すると、その内容を解析し、必要な情報項目を取り出した後、トランザクション証明19に登録要求a15を転送する。当該登録要求a15は、以下の様な構成を取る。

```
Transaction_Notary_Update::= {
  Transaction_Notary_Response;
  Entity_Identifier_Of_Sender;
  Entity_Identifier_Of_Receiver;
  Invocation_Time_At_Sender;
  Signature_Of_Sender;
  Key_Information;
};
```

当該登録要求a15は、ほぼ前述トランザクション証明応答a14と等価である。

【0109】

また、本実施の形態に係る電子商取引監査システムには、評価サイト5が含まれており、当該評価サイト5により、前述スコープA取引き監視サイト3および前述スコープB取引き監視サイト4からのトランザクションログの自動収集、および、当該トランザクションログに基づく監査が行われる。

【0110】

そこで、次に、この評価サイト5が関係する動作について説明する。

【0111】

評価サイト5にはトランザクションログ収集エージェント25が含まれており、これが定期的に前述の各スコープ取引き監視サイト内のトランザクションログにアクセスする。図1の例では、当該トランザクションログ収集エージェント2

5は、トランザクションログ17にアクセスし、前回収集からの差分に相当するトランザクションログ差分a16、すなわち、前述の時刻Tから時刻(T+Δ)までのトランザクションログを取り出す。トランザクションログ差分a16は、前述の時間間隔Δ毎に作成される前述トランザクションリストa12と同期が取れており、等価になる。当該トランザクションログ差分a16は、以下の様な構成を取る。

```
Transaction_Log_List ::= {
  Recieve_Confirmation [0];
  . . . . . . . . . . . . .
  Recieve_Confirmation [N];
};
```

上記のRecieve_Confirmationの配列の各々は、前述の受領確認a4に相当することになる。

【0112】

前述トランザクションログ収集エージェント25が、当該トランザクションログ差分a16を受け取ると、その内容の正当性を得る為、定められた方法で前述Transaction_Log_Listのダイジェスト計算を施し、その結果を検証要求a18として、前述公証エンティティa15に転送する。当該検証要求a18は、以下の様な構成を取る。

```
Transaction_Verification_Request ::= {
  Digest_Of_Transaction_Log_List;
  Signature_Of_Sender;
  Key_Information;
};
```

当該検証要求a18のDigest_Of_Transaction_Log_Listは、前述のダイジェスト計算の結果値である。対してSignature_Of_Senderは、この結果値に前述トランザクションログ収集エージェント25の秘密鍵で署名をしたものである。対して、当該検証要求a18内のKey_Informationは、当該秘密鍵に対応する公開鍵証明書に関する情報である。

【0113】

前述公証エンティティ15は、前述検証要求a18を受理すると、その内部の前述Signature_of_Senderに記述された署名値を検証し、送付者が前述トランザクションログ収集エージェント25であることを確認する。次に、前述検証要求a18内のダイジェスト計算の結果値である前述Digest_of_Transaction_Log_Listを取り出す。

【0114】

次に前述公証エンティティ15は、対応する登録情報を前述トランザクション証明19から引き出す為、参照要求a19を発行する。当該トランザクション証明19は、前述の登録要求a15に等価な形式で参照応答a20を前述公証エンティティ15に戻す。具体的には、トランザクションリストa12とトランザクションログ差分a16とは同期がとれていることから、トランザクション証明19は該当する時間間隔における情報を参照応答a20として戻すことが可能である。参照応答a20は、以下の様な構成を取る。

```
Transaction_Notary_Reference ::= {
  Transaction_Notary_Response;
  Entity_Identifier_of_Sender;
  Entity_Identifier_of_Receiver;
  Invocation_Time_At_Sender;
  Signature_of_Sender;
  Key_Information;
};
```

前述公証エンティティ15は、当該参照応答a20から、前述公証エンティティ16に代表される他の公証エンティティの署名であるSignature_of_Sender、並びに、その秘密鍵に対応する公開鍵証明書情報であるKey_Informationを取り出す。

【0115】

前述公開鍵証明書情報であるKey_Informationの形式は、特定されている訳ではない。その為、公開鍵そのものを含んだX.509V3形式の証明書そのもの

が記載されている場合もあるが、証明書情報の入手先であるアクセスポイントを U R I (Uniform Resource Identifier)形式等で記した場合もある。後者の場合、前述公証エンティティ15は、証明書入手要求a21を認証・登録局22に発行し、公開鍵そのものを含んだX.509V3形式の証明書a22を入手する。

【0116】

その後、前述公証エンティティ15は、取り出した前述Signature_of_Senderを、入手した証明書に付与された公開鍵で復号計算し、前述トランザクション証明19に記載されたダイジェスト値を求める。その後、当該ダイジェスト値を前述検証要求a18内のダイジェスト計算結果値である前述Digest_of_Transaction_Log_Listと比較する。当該公証エンティティ15は複数の他公証エンティティと相互公証の交換を行う為、当該ダイジェスト値の比較処理は、前述トランザクション証明19に保存された前述参照応答a20全てに対して成される。

【0117】

前述参照応答a20の何れの場合でも、ダイジェスト値の比較で差違が認められないことが確認出来たならば、前述公証エンティティ15は、前述トランザクションログ収集エージェント25に対して、検証応答a23を戻す。当該検証応答a23は、以下の様な構成となる。

```
Transaction_Verification_Response ::= {
  Boolean_Verified;
}
```

当該Boolean_Verifiedは、問題が無い場合は”True”が戻され、それ以外の場合は”Failure”が戻される。

【0118】

前述トランザクションログ収集エージェント25は、当該検証応答a23を受け、前述Boolean_Verifiedに”True”を確認した場合、前述評価サイト5内で管理しているスコープAトランザクションログ26にエントリを追加・作成する為の要求コマンドa17を呼び出す。

【0119】

当該スコープAトランザクションログ26は、前述トランザクションログ差分

a 16 だけではなく、前述トランザクションログ17 の内、定められた有効期間内の全受領確認 a 4 を含む。

【0120】

同じ要領で前述トランザクションログ収集エージェント25 は、全てのスコープ取引き監視サイトからトランザクションログを取り出し、前述トランザクションログ26 と同様に、前述トランザクションログ26' 、前述トランザクションログ26" を作成する。

【0121】

評価サイト5 には、プロトコル標準収集エージェント27 も含まれており、これが定期的にプロトコル標準を管理する複数のプロトコル標準管理リポジトリサイト23 、24 からプロトコル記述の最新版記述 a25 、 a26 を取り出す。前述プロトコル標準管理リポジトリサイトA23 は、RosettaNet のリポジトリに相当し、プロトコル記述の最新版記述 a25 はPIP 定義等に相当する。PIP 定義等の様にドキュメントで記されているプロトコルの記述の最新版情報は、前述プロトコル標準収集エージェント27 がコンソールを持つ為、人間を介した編集・メンテナンスで処理される。

【0122】

前述プロトコル標準収集エージェント27 は、前述プロトコル記述の最新版記述 a25 、 a26 を引数として、プロトコル記述の最新版情報生成コマンド a27 、 a28 を発行することで、前述評価サイト5 の内部にトランザクション定義 A30 、並びにトランザクション定義 B29 に関するテーブルを構築する。当該トランザクション定義 A30 、並びに当該トランザクション定義 B29 は、以下の様な構成を持つオートマトンの定義表、並びにメッセージの構成表群である。

```
Transaction_Definition_Table ::= {
  Category_Of_Message;
  Current_Status_Definition;
  Input_Event_Category; (MessageSending, OtherEvent)
  SubCategory_Of_Message; (Input)
  Message_Definition; (Input)
}
```

```

Next_Status_Definition;
Output_Event_Category; (MessageSending,OtherEvent)
SubCategory.Of_Message; (Output)
Message_Definition; (Output)
};

Message_Table::= {
  Definition of Structure in BNF ;
};

```

当該Transaction_Difinition_Table内のCategory.Of_Messageは、やり取りするメッセージの種類を意味する、例えばRosettaNet等が相当する。当該Transaction_Difinition_Table中のCurrent_Status_Definition、Next_Status_Definitionは、前述電子商取引エンティティ11、12、13、14が各種メッセージ通信の手続き中にソフトウェア的に持ち得る状態を意味し、Current_Status_Definitionは遷移前の状態、Next_Status_Definitionは遷移後の状態を意味する。

【0123】

当該Transaction_Difinition_Table内のInput_Event_Category、Output_Event_Categoryは、前述電子商取引エンティティ11、12、13、14が各種メッセージ通信の手続き中に受け入れられるイベントの全てであり、Input_Event_Categoryは、状態遷移を引き起こし得るイベントを定義し、Output_Event_Categoryは、状態遷移の結果、生じるイベントを定義する。

【0124】

Transaction_Difinition_Table内のSubCategory.Of_Message、Message_Definitionは、具体的なメッセージの種類とその構文を定義する。

【0125】

Message_Tableでは、前述Message_Definitionを定義する為の記述をBNF(Baekus-Naur Form)で記したものである。

【0126】

通常、当該トランザクション定義A29、当該トランザクション定義B30を

始めとする各種トランザクション定義は、評価サイト5内のログ解析エンジン28配下の巨大なメモリ空間に展開され、`Transaction_Definition_Table`参照、`Message_Table`参照 a29、a30により参照されることになる。

【0127】

前述ログ解析エンジン28は常時、起動・運転されており、各前述電子商取引エンティティ11、12、13、14の状態シュミレーションを行う。

【0128】

当該ログ解析エンジン28は、前述のトランザクション定義A29、トランザクション定義B30を参照し、`Transaction_Definition_Table`内の要素である、前述`Category_of_Message`、前述`Current_Status_Definition`、前述`Input_Event_Category`、前述`SubCategory_of_Message`、前述`Message_Definition`、前述`Next_Status_Definition`、前述`Output_Event_Category`、並びに`Message_Table`内の要素である前述`Definition of Structure in BNF`に関する定義情報を読み込む。

【0129】

その後、前述ログ解析エンジン28は、前述トランザクションログ26、26'、26"を統合し、当該ログ解析エンジン28配下の巨大なメモリ空間に、下記のデータ構造`Transaction_Group_Table`を構築し、これが`Transaction_Group_Table`参照 a24により参照されることになる。

```
Transaction_Group_Table ::= {
  Transaction_Identifier;
  List_of_Trace_Structure;
  Status; (Complete, Still_In_Progress)
};

Trace_Structure ::= {
  Entity_Identifier_of_Sender;
  Entity_Identifier_of_Receiver;
  Category_of_Message;
  Identifier_of_Message;
  Time_Stamp_Value;
};
```

};

当該データ構造Transaction_Group_Tableは、Transaction_Identifierを主キーに、個々のメッセージ転送をTransaction_Group_Tableとして束ねたもの、並びに当該メッセージ転送の具体的な内容を意味するTrace_Structure、並びに、その一連のトランザクションの状態を意味する状態Statusから構成される。

【0130】

その後、前述ログ解析エンジン28は、同じTransaction_Identifierを持つTrace_Structureから、図2に示す様な配列を成す有向グラフモデルをメモリ上で生成する。Transaction_Identifierを選択する際には、前述Statusが”Still_In_Progress”の値を持つもののみが対象となる。この配列を成す有向グラフモデルは、式(1)、式(2)、式(3)、式(4)で定義される。

【0131】

【数1】

$$\begin{aligned}
 & (e_n(t_v), e_m(t_u), D) \in \text{Set of Message} \quad (1) \\
 & e_n(t_v), e_m(t_u) \in \text{Set of Entity_Identifier} \\
 & (\forall n, \exists m \ \& n \neq m \ \& n, m < \infty) \text{ at } t_v, t_u \quad (2) \\
 & t_v, t_u \in \text{Set of Time Stamp} \\
 & (\forall v, \exists u \ \& \{(v < u \text{ when } D = " \rightarrow ") \mid| (v > u \text{ when other})\}) \quad (3) \\
 & D \in \{" \rightarrow ", " \leftarrow "\} \quad (4)
 \end{aligned}$$

図2の配列100からなるグラフ上のノード101は、電子商取引エンティティのいずれかに相当し、当該電子商取引エンティティは、式(2)で定義された前述Trace_StructureのEntity_Identifier_of_Sender、もしくはEntity_Identifier_of_ReceiverのEntity_Identifierによって特定される。配列の各メンバ102、103は各メッセージ転送の授受する時刻であるTime_Stampを表示している。当該各メンバ102、103間のアーカ104は、メッセージ転送の方向を意味する。

【0132】

前述ログ解析エンジン28における監査解析は、図3の手順に従う。

【0133】

第1ステップとして、電子商取引エンティティの一つに着目し、その実装の仕様準拠性を監査する。その為に、まず、図2の有向グラフの例えばノード101に着目し、対応する配列100を取り出す。そして、この配列100の各メンバについて、紐付けられたアーケークの方向、初期状態、並びに、その種類に基づき、Transaction_Definition_Table参照、Message_Table参照a29、a30により、該当する前述Current_Status_Definition、並びに次状態である前述Next_Status_Definitionの特定を試みる。

【0134】

これは、数式で記すと、式(5)、式(6)、式(7)、式(8)で表現される順序集合を電子商取引エンティティ毎に特定することに相当する。

【0135】

【数2】

$\{\text{Status}(e_n(t_1)), \text{Status}(e_n(t_2)), \dots, \text{Status}(e_n(t_x))\}$ (5)

$\text{Status}(e_n(t_x)) \in \text{Set of Status at } e_n(t_x) \ (\forall n, n < \infty) \text{ at } t_x$ (6)

$e_n(t_x) \in \text{Set of Entity_Identifier} \ (\forall n, n < \infty) \text{ at } t_x$ (7)

$t_x \in \text{Set of Time Stamp} \ (0 < x < \infty)$ (8)

もし、式(5)で表現される順序集合をTransaction_Identifierの死滅段階迄、導出出来る場合は、図2中の該当するノード101に対応する電子商取引エンティティについては、検証されたトランザクションに関する限り、実装上の問題がないことが証明されることになる。

【0136】

その後、前述ログ解析エンジン28は、累積評価管理部31に、当該電子商取引エンティティの識別子を指定することで、現時点迄の電子商取引エンティティの監査結果記録a31を取り出す。そして、今回の証明結果を定められたアルゴリズムを用いて反映した後、最新監査結果記録a32として前述累積評価管理部31に戻す。

【0137】

前述ログ解析エンジン28は、全ての電子商取引エンティティ相当のノードで、上記を実施し、第1ステップを完了させる。

【0138】

第2ステップとして、前述ログ解析エンジン28は、電子商取引エンティティの一つに着目し、その応答反応能力を監査する。特に、金融関係情報を扱う場合は、不渡可能性検証も監査する。その為に、図2の有向グラフ中のあるノード101の配列を取り出し、式(9)に示された条件を満足する一連の Δt を計算で求め、順序集合を作成する。

【0139】

【数3】

$$\begin{aligned} \Delta t &= t_x - t_y, \\ (t_x : (e_n(t_x), e_m(t_u), " \leftarrow ") &\in \text{Set of Message} \ \& \\ t_y : (e_n(t_y), e_m(t_u), " \rightarrow ") &\in \text{Set of Message} \end{aligned} \quad (9)$$

上記 Δt とは、ある電子商取引エンティティが、要求メッセージを受け取った後に、その応答メッセージを戻す迄の時間であり、その電子商取引エンティティの処理能力を記す、一つの目安になる。特にそれらメッセージが、金融関係の情報を扱う場合、メッセージの種類を特定することで、不渡可能性の有無を推定することも可能となる。

【0140】

その後、前述ログ解析エンジン28は、累積評価管理部31に、当該電子商取引エンティティの識別子を指定することで、現時点迄の電子商取引エンティティの応答反応能力・不渡可能性検証記録a37を取り出す。そして、今回の監査結果を定められたアルゴリズムを用いて反映した後、最新応答反応能力・不渡可能性検証記録a38として前述累積評価管理部31に戻す。

【0141】

前述ログ解析エンジン28は、全ての電子商取引エンティティ相当のノードで、上記を実施し、第2ステップを完了させる。

【0142】

第3ステップとして、前述ログ解析エンジン28は、電子商取引エンティティの一つに着目し、その電子商取引エンティティが発する異常応答処理比率を監査する。その為に、図2の有向グラフ中のあるノード101の配列を取り出し、式

(10) 以下に示された条件を満足する頻度を計算する。

【0143】

【数4】

```
if (Req(en(tx), em(tu), "←") && Err(en(ty), em(tu), "→")) {True;}
else if (Req(en(tx), em(tu), "←") && Res(en(ty), em(tu), "→")) {Failure;}
else {Failure;} (10)
```

Definition of Function Req :

∀m : m=(e_n(t_x), e_m(t_u), "←") ∈ Set of Message

mのカテゴリが、"要求"の場合、Req(m)=True; (11)

Definition of Function Res :

∀m : m=(e_n(t_x), e_m(t_u), "→") ∈ Set of Message

mのカテゴリが、"正常応答"の場合、Res(m)=True; (12)

Definition of Function Err :

∀m : m=(e_n(t_x), e_m(t_u), "→") ∈ Set of Message

mのカテゴリが、"異常応答"の場合、Err(m)=True; (13)

前述の式(11)、式(12)、式(13)は、関数定義式であり、式(11)では、扱うメッセージの種類が"要求"相当のものであれば、"真"とする。式(12)では、扱うメッセージの種類が"正常応答"相当のものであれば、"真"とする。式(13)では、扱うメッセージの種類が"異常応答"相当のものであれば、"真"とする。

【0144】

前述の式(10)の意味は、異常応答を発生させる頻度計算の為の条件定義である。当該頻度が高い場合は、電子商取引エンティティが接続する、応用システム上で問題があることが推定される。長期的にこの頻度をトレースすることで、問題点を明確化することが出来る。

【0145】

その後、前述ログ解析エンジン28は、累積評価管理部31に、当該電子商取引エンティティの識別子を指定することで、現時点迄の電子商取引エンティティの異常応答処理比率監査記録a39を取り出す。そして、今回の監査結果を定められたアルゴリズムを用いて反映した後、最新異常応答処理比率監査記録a40

として前述累積評価管理部31に戻す。

【0146】

前述ログ解析エンジン28は、全ての電子商取引エンティティ相当のノードで上記を実施し、第3ステップを完了させる。

【0147】

前述ログ解析エンジン28は、前述第1ステップ、第2ステップ、第3ステップを実施した後、前述の有向グラフモデルをメモリ上から消去し、前述Transaction_Group_Table参照a24により得たTransaction_Group_Tableの該当Transaction_IdentifierのStatusを”Complete”に書き換える。その後、前述Transaction_Group_Table参照a24により、前述Statusが”Still_In_Progress”的値を持つもので、次のTransaction_Identifierに相当するTrace_Structureから、前述同様、有向グラフモデルをメモリ上に生成し直す。前述Transaction_Group_Table参照a24から、適切なTransaction_Identifierを取り出せない場合は、Transaction_Group_Table参照a24をリフレッシュし、次の処理ラウンドに進む。

【0148】

図1の企業D9上に実装された電子商取引エンティティ14が、他社との電子商取引の開始に応じて、他電子商取引エンティティとメッセージ通信を行う場合は、前述評価サイト5の監査情報サービス32に監査サービス情報提供要求a33を送付する。当該監査サービス情報提供要求a33は、下記の様な構成を取る。

```
Inspection_Service_Request::= {
  Entity_Identifier_Of_Requester;
  Entity_Identifier_Of_Opposite;
  Signature_Of_Requester;
  Key_Information;
};
```

当該監査サービス情報提供要求a33のEntity_Identifier_Of_Requesterは、前述電子商取引エンティティ14に関するアクセスポイントを意味し、国際規約団体W3C等で定められたURI(Uniform Resource Identifier)等で記述され

る。対して、Entity_Identifier_of_Oppositeは評価・査定先の電子商取引エンティティに関するアクセスポイントを意味し、同様にURI(Uniform Resource Identifier)等で記述される。

【0149】

当該監査サービス情報提供要求a33のSignature_of_Requesterは、当該Inspection_Service_Requestの前述Entity_Identifier_of_Requester、並びに前述Entity_Identifier_of_Oppositeに、前述電子商取引エンティティ14の秘密鍵で署名をしたものである。対して、Key_Informationは、当該秘密鍵に対応する公開鍵証明書に関する情報である。

【0150】

前述監査情報サービス32は、当該監査サービス情報提供要求a33を受理すると、署名である前述Signature_of_Requesterを検証し、前述電子商取引エンティティ14からの要求であることを確認した後、前述Entity_Identifier_of_Oppositeを取り出す。その後、前述の累積評価管理部31に、当該Entity_Identifier_of_Oppositeを引数として問い合わせ要求a34を発行する。

【0151】

前述累積評価管理部31は、Entity_Identifier_of_Oppositeで記される電子商取引エンティティに関する、前述最新監査結果記録a32、前述最新応答反応能力・不渡可能性検証記録a38、前述最新異常応答処理比率監査記録a40を纏めた問い合わせ応答a35を作成し、前述監査情報サービス32に回答する。

【0152】

その後、前述監査情報サービス32は、前述電子商取引エンティティ14に監査サービス情報提供応答a36を回答する。この監査サービス情報提供応答a36は下記の様な構成を取る。

```
Inspection_Service_Response::= {
  Entity_Identifier_of_Requester;
  Entity_Identifier_of_Opposite;
  Inspection_Item[1];
  Inspection_Item[2];
}
```

Inspection_Item[3];

Signature_of_Respondent

Key_Information;

};

当該監査サービス情報提供応答 a 3 6 のEntity_Identifier_of_Requester、Entity_Identifier_of_Oppositeは、当該監査サービス情報提供要求 a 3 3 のそれらと同じである。当該監査サービス情報提供応答 a 3 6 のInspection_Itemの各々は、前述最新監査結果記録 a 3 2、前述最新応答反応能力・不渡可能性検証記録 a 3 8、前述最新異常応答処理比率監査記録 a 4 0 を意味する。

[0 1 5 3]

当該監査サービス情報提供応答 a 3 6 のSignature_of_Responderは、当該Inspection_Service_Responseの前述Signature_of_Responder、前述Key_Information以外を、前述評価サイト 5 の秘密鍵で署名をしたものである。対して、Key_Informationは、当該秘密鍵に対応する公開鍵証明書に関する情報である。

[0 1 5 4]

以上により、本実施の形態に係る電子商取引監査システムの処理が終了する。

[0 1 5 5]

次に本発明の第2の実施の形態を図面を参照して説明する。

[0 1 5 6]

図4を参照すると、本実施の形態は、上記第1の実施の形態の構成に加え、さらに、記録媒体41および42を含んでいる。ここで、図4においては、図面作成の都合上、詳細な構成および情報の流れは省略してあるが、図示された各構成要素は、図1に示したものと同様の構成を有するものとし、各構成の間でやり取りされる情報も図1に示したものと全く同じである。図4において、記録媒体41には、スコープA取引き監視サイト3またはスコープB取引き監視サイト4が行うべき処理を実行するためのプログラムが記録されており、記録媒体42には、評価サイト5が行うべき処理を実行するためのプログラムが記録されている。スコープA取引き監視サイト3またはスコープB取引き監視サイト4は、記録媒

体41からロードされたプログラムによる制御の下、評価サイト5は、記録媒体42からロードされたプログラムによる制御の下、それぞれ、上記第1の実施の形態と同様の処理を行う。なお、記録媒体41および42は、磁気ディスク、半導体メモリその他の記録媒体であってよく、また、プログラムは複数の記録媒体からなる記録媒体群に分割して記録されていてもよい。

【0157】

【発明の効果】

次に、本発明の効果について述べる。

【0158】

従来方式に起因して顕在化する問題1とは、広域なネットワーク領域を捉えて、事象の検証を行う監査が不可能なことであった。

【0159】

この問題については、複数の電子公証機能で分散されて公証・記録された電子商取引全ての交換メッセージを自動的に収集し、広域なネットワーク領域全体の事象として再現するトランザクションログ収集エージェント機能、および、電子商取引の仕様規約を自動的に収集し、それにより広域なネットワーク領域全体で起こるべき事象を正しく把握するプロトコル標準収集エージェント機能、および、前述トランザクションログ収集エージェント機能により再現される、前述の広域ネットワーク領域全体の事象、並びに前述プロトコル標準収集エージェント機能により把握される前述広域ネットワーク領域全体で起こるべき事象、との両者を比較することで、客観的監査を実施するログ解析エンジンにより、広域なネットワーク領域を捉えて、事象の検証を行う監査が可能となる為、解決出来ることになる。

【0160】

従来方式に起因して顕在化する問題2とは、メッセージの内容を判断して、監査を行うことが出来ないことであった。

【0161】

この問題についても、複数の電子公証機能で分散されて公証・記録された電子商取引全ての交換メッセージを自動的に収集し、広域なネットワーク領域全体の

事象として再現するトランザクションログ収集エージェント機能、および、電子商取引の仕様規約を自動的に収集し、それにより広域なネットワーク領域全体で起こるべき事象を正しく把握するプロトコル標準収集エージェント機能、および、前述トランザクションログ収集エージェント機能により再現される、前述の広域ネットワーク領域全体の事象、並びに前述プロトコル標準収集エージェント機能により把握される前述広域ネットワーク領域全体で起こるべき事象、との両者を比較することで、客観的監査を実施するログ解析エンジンにより、広域なネットワーク領域を捉えて、事象の検証を行う監査が可能となる為、解決出来ることになる。

【0162】

従来方式に起因して顕在化する問題3とは、監査人や、システム自体の信頼性保証の考え方がなく、重大な記録を漏洩し得る可能性が存在することであった。

この問題については、時刻を統一的に打刻し、電子商取引上の交換メッセージ全てを記録・保存する複数の電子公証機能、および、当該電子公証機能間で、前述記録・保存されている交換メッセージ全ての相互公証を取り合う機能により解決出来ることになる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態のシステム構成を示すブロック図である。

【図2】

本発明の第1の実施の形態において、同一Transaction_Identifierを持つTrace_Structureから、メモリ上に生成される配列を成す有向グラフモデルに関する図である。

【図3】

本発明の第1の実施の形態における監査手順を示す流れ図である。

【図4】

本発明の第2の実施の形態のシステム構成を示すブロック図である。

【図5】

従来発明の通信監査装置、および通信監査方法に係る暗号通信システムを示す

概念図である。

【図6】

従来実施形態で転送対象となるパケットの一例としてTCP/IPパケットの構造を示した図である。

【図7】

従来発明の通信監査装置による監査の概要を記した図である。

【図8】

従来発明の通信監査装置の内部構成の一例を示す。

【符号の説明】

1…スコープA、2…スコープB、3…スコープA取引き監視サイト、4…スコープB取引き監視サイト、5…評価サイト、6…企業A、7…企業B、8…企業C、9…企業D、11…電子商取引エンティティ、12…電子商取引エンティティ、13…電子商取引エンティティ、14…電子商取引エンティティ、15…公証エンティティ、16…公証エンティティ、17…トランザクションログ、18…トランザクションログ、19…トランザクション証明、20…トランザクション証明、21…タイムスタンプサーバ、22…認証・登録局、23…プロトコル標準管理リポジトリサイトB、24…プロトコル標準管理リポジトリサイトA、25…トランザクションログ収集エージェント、26…トランザクションログ、26'…トランザクションログ、26''…トランザクションログ、27…プロトコル標準収集エージェント、28…ログ解析エンジン、29…トランザクション定義B、30…トランザクション定義A、31…累積評価管理部、32…監査情報サービス、41…記録媒体、42…記録媒体

a1…タイムスタンプ要求、a2…時刻要求、a3…時刻値応答、a4…受領確認、a5…タイムスタンプ応答、A6…要求メッセージ、a7…タイムスタンプ要求、a8…時刻要求、a9…時刻値応答、a10…受領確認、a11…タイムスタンプ応答、a12…トランザクションリスト、a13…トランザクション証明要求、a14…トランザクション証明応答、a15…登録要求、a16…トランザクションログ差分、a17…要求コマンド、a18…検証要求、a19…参照要求、a20…参照応答、a21…証明書入手要求、a22…X.509V

3形式の証明書、a23…検証応答、a24…Transaction_Group_Table参照、a25…プロトコル記述の最新版記述、a26…プロトコル記述の最新版記述、a27…プロトコル記述の最新版記述生成コマンド、a28…プロトコル記述の最新版記述生成コマンド、a29…Transaction_Definition_Table参照、Message_Table参照、a30…Transaction_Definition_Table参照、Message_Table参照、a31…電子商取引エンティティの監査結果記録、a32…最新電子商取引エンティティの監査結果記録、a33…監査サービス情報提供要求、a34…問い合わせ要求、a35…問い合わせ応答、a36…監査サービス情報提供応答、a37…応答反応能力・不渡可能性検証記録、a38…最新応答反応能力・不渡可能性検証記録、a39…異常応答処理比率監査記録、a40…最新異常応答処理比率監査記録

100…配列、101…グラフ上のノード、102…配列の各メンバ、103…配列の各メンバ、104…アーク

111…内部ネットワーク、112…外部ネットワーク、120…通信監査装置

121…送信元のアドレス、122…送信先のアドレス、123…プロトコルの種類（ポート番号）、124…データの内容

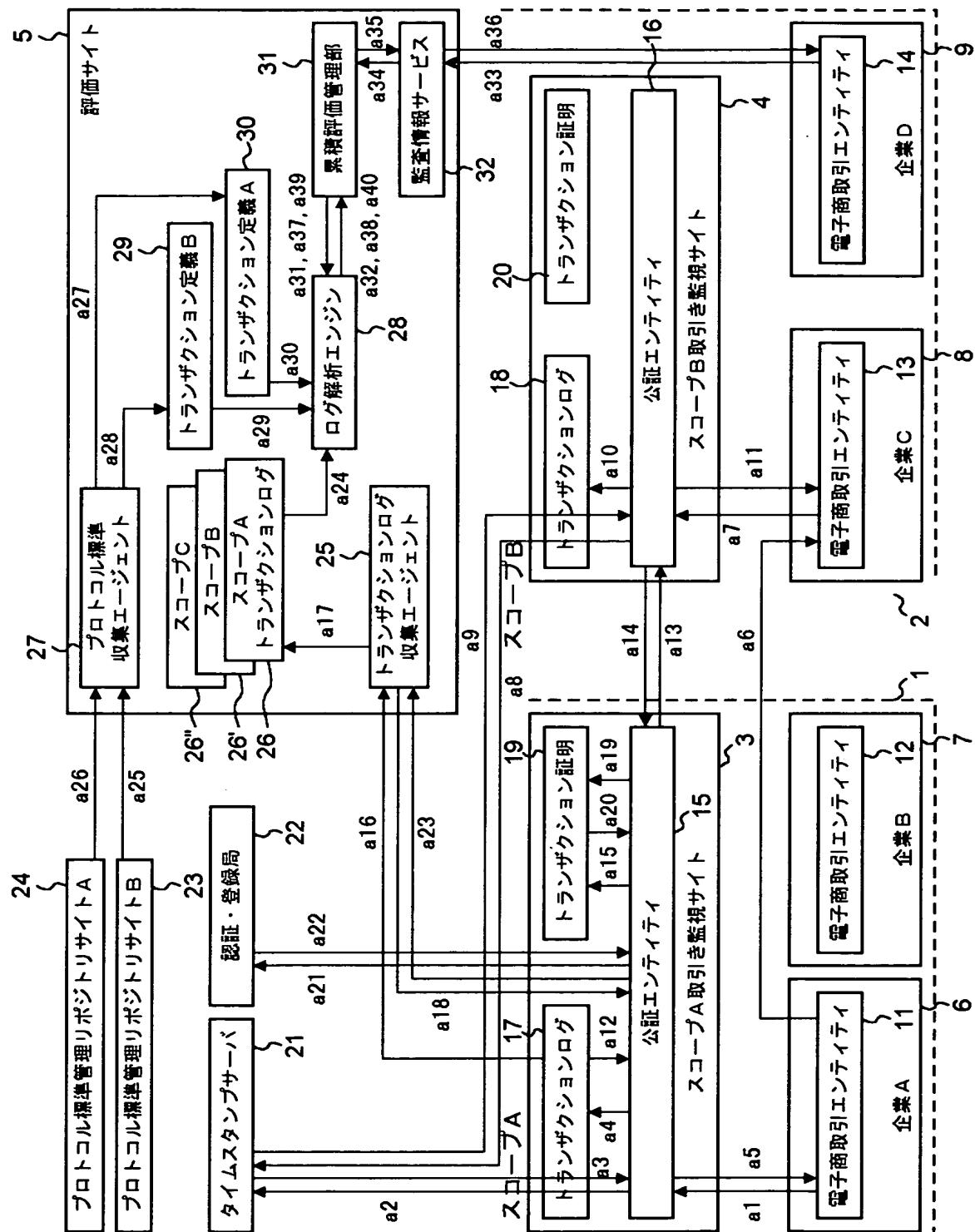
120…通信監査装置

141…ユーザBからの暗号メール、142…送信されるパケットに含まれる情報の概略、143…パケット解析部、145…送信ログ取得部、146…送信パケット統計処理部、147…監査条件判定部、148…メール発信部、149…警告メッセージ発信部

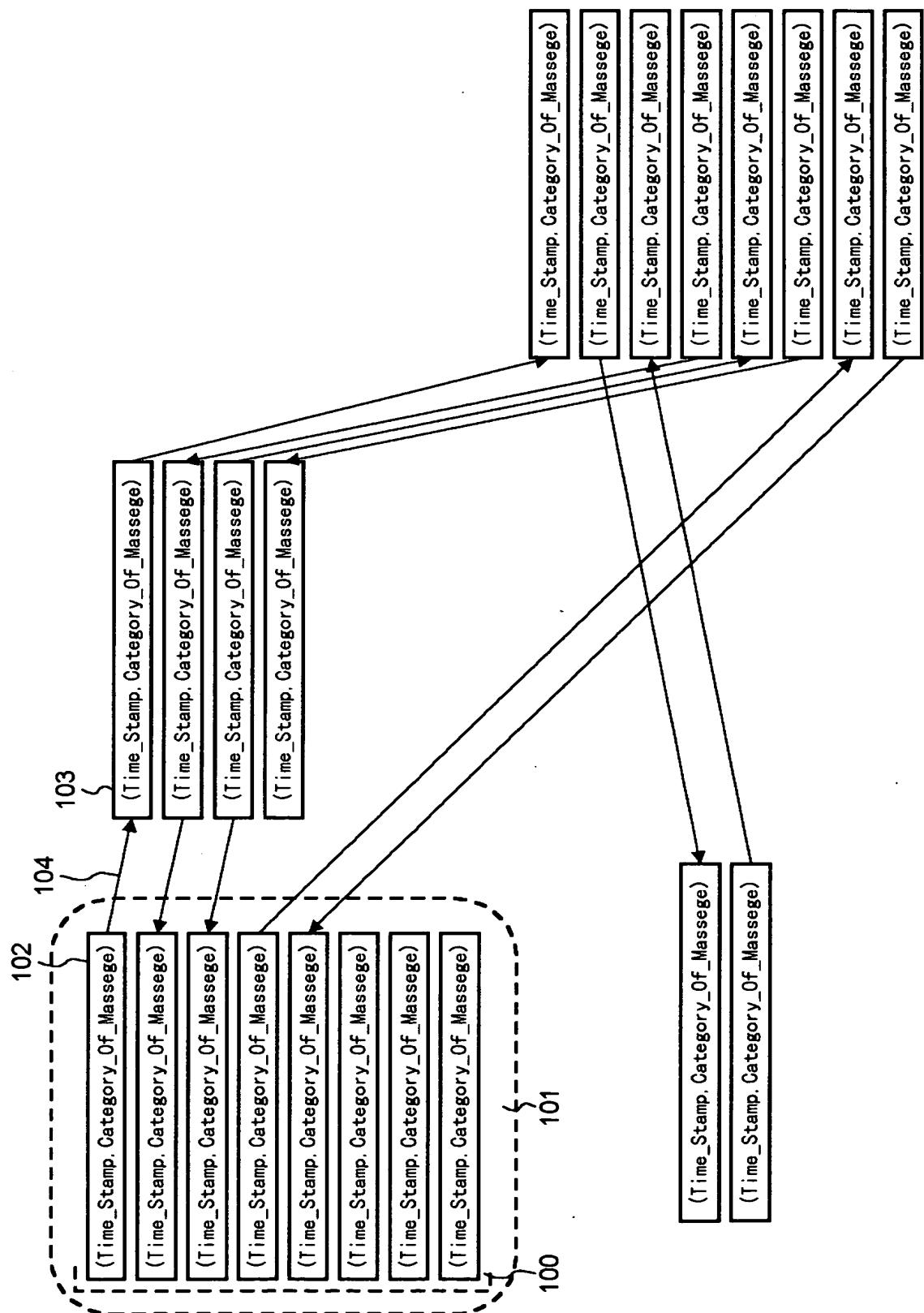
【書類名】

圖面

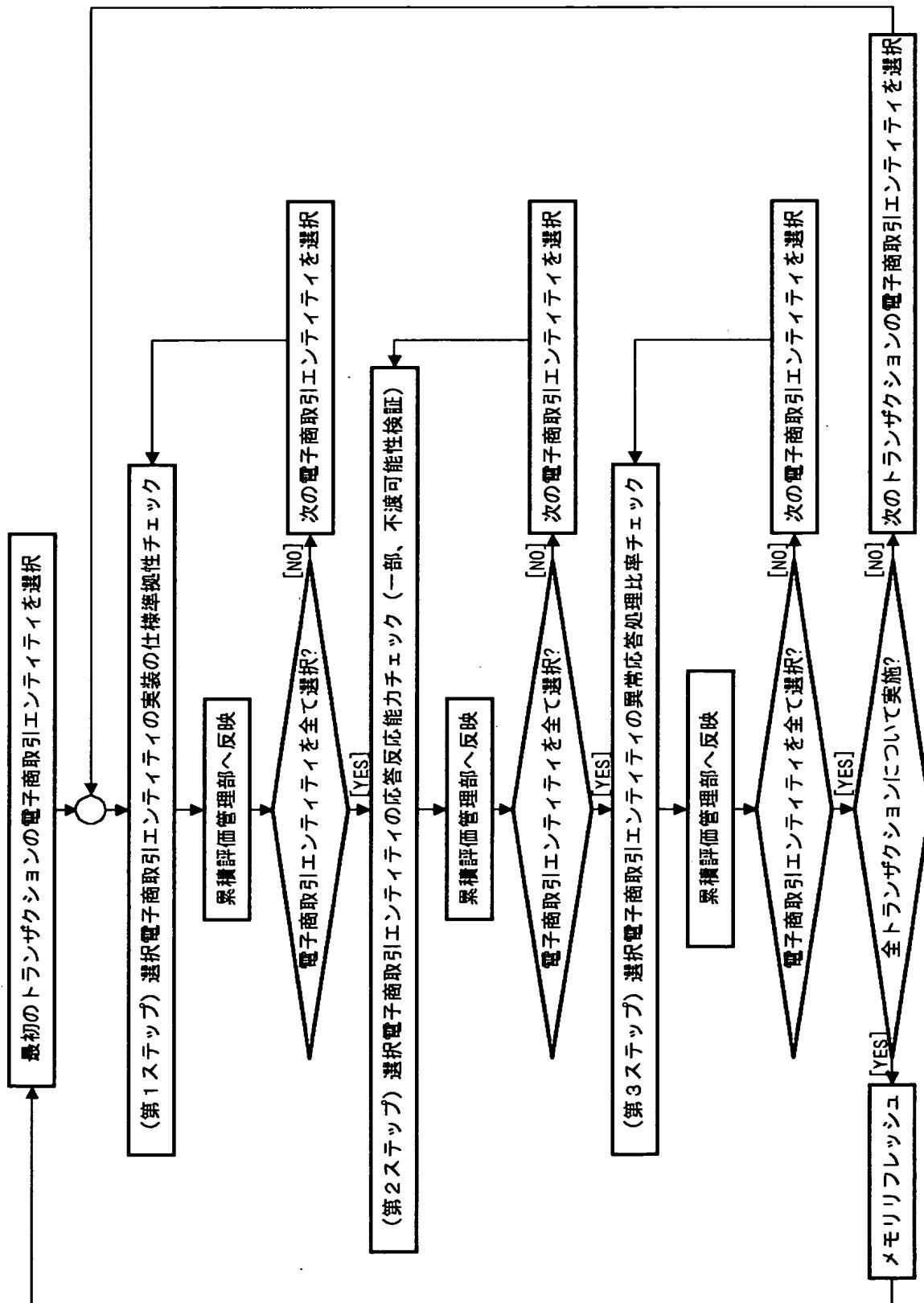
[図 1]



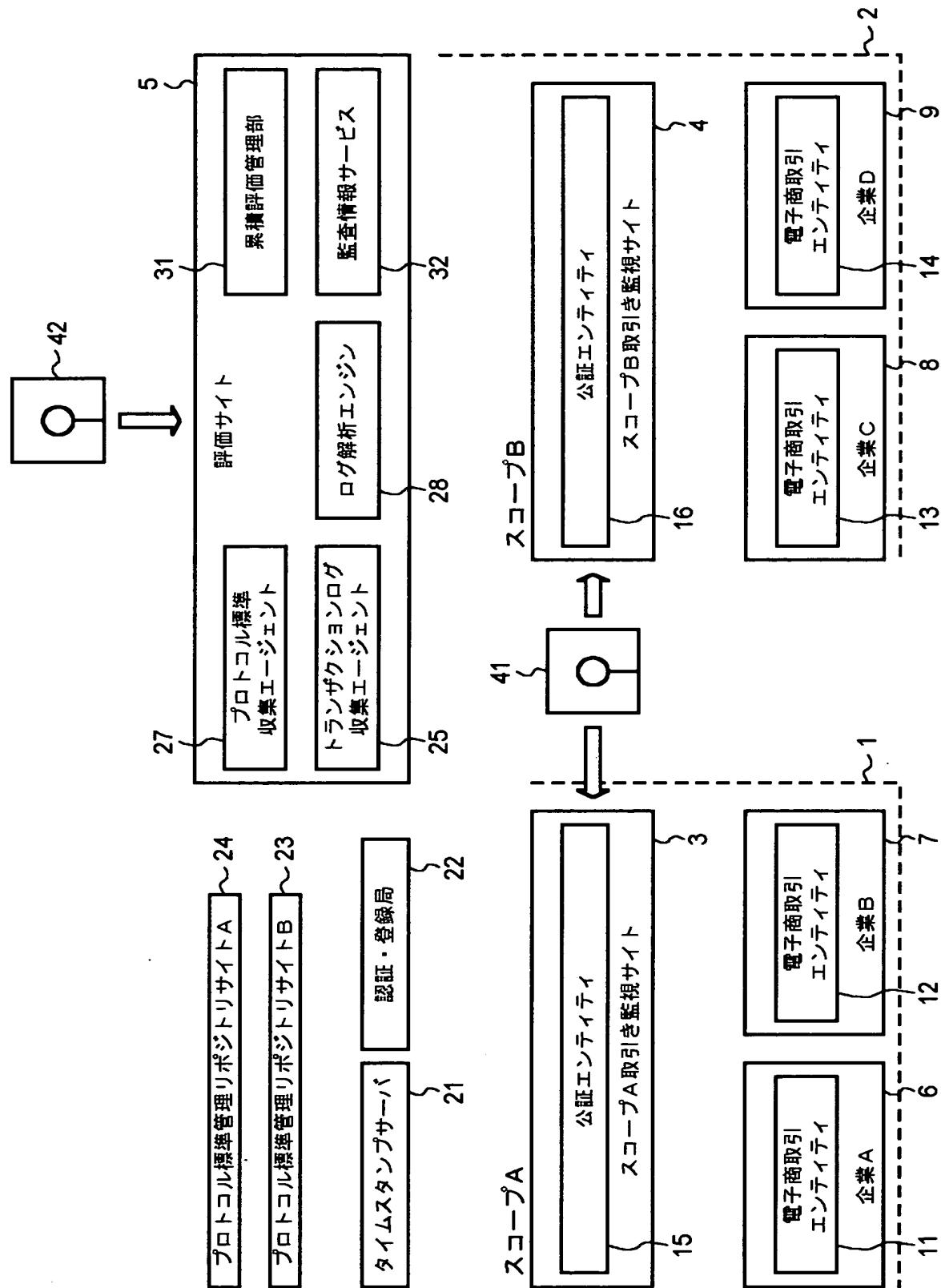
【図2】



【図3】



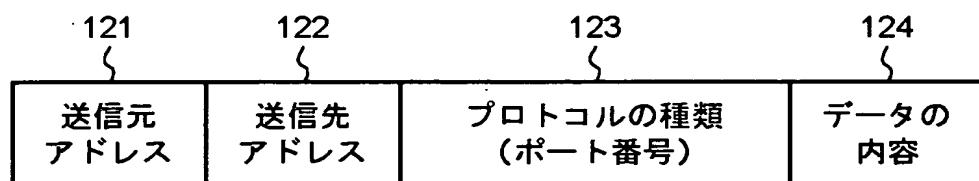
【図4】



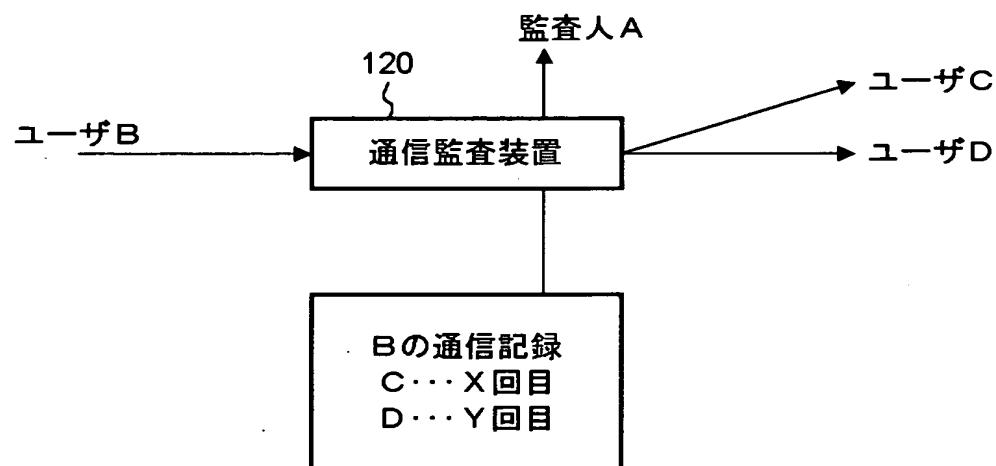
【図5】



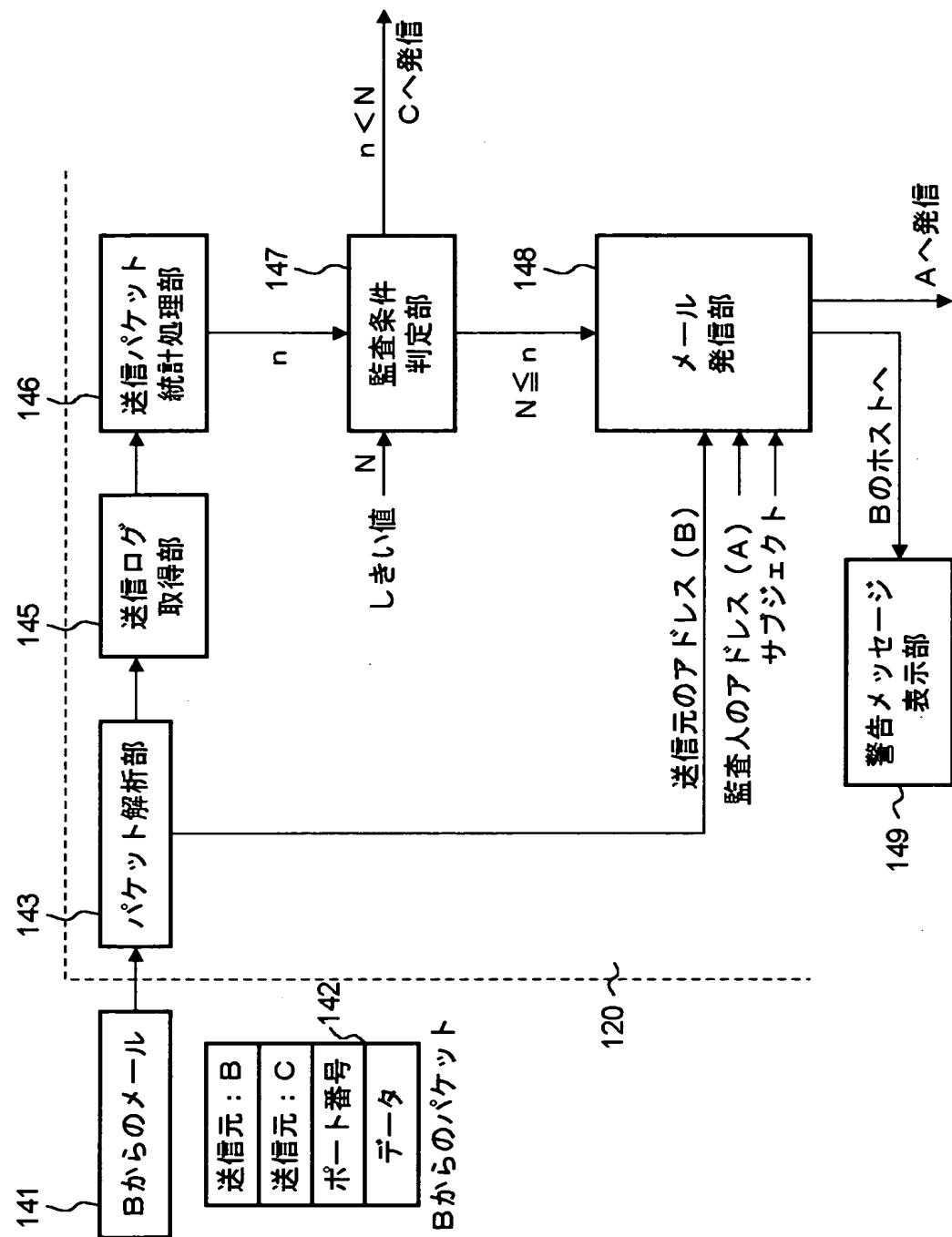
【図6】



【図7】



【図8】



【書類名】 要約書

【要約】

【課題】 メッセージ交換用の計算機がネットワーク接続された環境下で、各計算機が電子商取引の仕様を満足しているか、処理能力に問題がないかを監査する。

【解決手段】 電子商取引上の交換メッセージに時刻を統一的に打刻し記録・保存する複数の電子公証機能と、当該電子公証機能の間で記録・保存される全ての交換メッセージの相互公証を取り合う機能と、当該電子公証機能で公証・記録された全ての交換メッセージを自動的に収集しネットワーク領域全体の事象として再現するトランザクションログ収集エージェント機能と、電子商取引の仕様規約を自動的に収集しネットワーク領域全体で起こるべき事象を正しく把握するプロトコル標準収集エージェント機能と、前述再現されたネットワーク領域全体の事象と前述プロトコル標準収集エージェント機能で把握されたネットワーク領域全体で起こるべき事象とを比較して客観的監査を行うログ解析エンジンとを備える。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2000-298939
受付番号	50001264785
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年10月 3日

＜認定情報・付加情報＞

【提出日】 平成12年 9月29日

次頁無

出願人履歴情報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号

氏 名 日本電気株式会社